Serial No.: 09/943,720

1   LISTING OF CLAIMS

2   We claim:

3   1. (currently amended) A method comprising:

4   providing a data processing operation involving at least one lookup table, each particular
5   table from said at least one lookup table having a particular lookup table size and a particular
6   lookup table index size; and

7   creating at least one randomized table in which entries and/or indices are statistically
8   independent from entries and/or indices of said at least one lookup table, each individual table
9   from said at least one randomized table having a randomized table size, wherein a first sum of
10   sizes of all said randomized tables is smaller than a second sum of sizes of all lookup tables, or
11   the maximum index size of said randomized tables is less than the maximum index size of the
12   lookup tables, wherein the step of creating said at least one randomized table includes applying a
13   Table Masking operation to at least one of said lookup tables and/or to split lookup tables
14   resulting in masked tables.

15   2. (original) A method as recited in claim 1, further comprising performing said data processing
16   operation employing said at least one randomized table.

17   3. (original) A method as recited in claim 1, wherein the step of providing includes obtaining
18   said data processing operation.

19   4. (original) A method as recited in claim 1, wherein the step of creating said at least one
20   randomized table includes applying a Table Split operation to at least one of said lookup tables
21   resulting in split lookup tables; and/or applying a Table Masking operation to at least one of said
22   lookup tables and/or split lookup tables resulting in masked tables.

DOCKET NUMBER: YOR20010711US2   3/25

Serial No.: 09/943,720

1   5. (canceled) .

2   6. (currently amended) A method as recited in claim 1 5, wherein the step of creating said at

3   least one randomized table includes the step of applying a Table Aggregate operation to at least

4   one of said masked tables.

5   7. (original) A method as recited in claim 4, wherein the step of applying a Table Split operation

6   includes employing a Two-way Byte Table Splitting Method.

7   8. (currently amended) A method as recited in claim 1 5, wherein the step of applying a Table

8   Mask operation includes employing a Input-Output Permutation Masking Method.

9   9. (original) A method as recited in claim 6, wherein the step of applying a Table Aggregate

10   operation includes employing an Entry-wise Algebraic Aggregate Method.

11   10. (original) A method as recited in claim 1, wherein said at least one table is a table from a

12   COMP128 application.

13   11. (original) A method as recited in claim 1, wherein a number of elements in said at least one

14   lookup table is given by a power of two.

15   12. (original) A method as recited in claim 1, further comprising:

16   employing said at least one randomized table in a cryptographic process;

17   applying said at least one randomized table for securely handling information in said

18   cryptographic process.

19   13. (original) A method as recited in claim 12, further comprising:

DOCKET NUMBER: YOR20010711US2   4/25

Serial No.: 09/943,720

1   prior to performing said cryptographic process, transforming the information by applying

2   a secret-sharing operation to the elements of the information where each element of the

3   information is related to multiple elements of the transformed information;

4   performing the cryptographic process on the transformed information involving the use of

5   said randomized table; and

6   retransforming the transformed and cryptographically processed information by applying

7   an inverse secret-sharing operation to the transformed and cryptographically processed

8   information.

9   14. (currently amended) A method as recited in claim 1 5, wherein indices to at least one masked

10   table of said plurality of masked tables are masked by a single permutation and data values in

11   said at least one masked table are masked by a single permutation.

12   15. (original) A method as recited in claim 1, further comprising employing the data processing

13   operation as a countermeasure against at least one first-order side-channel attack.

14   16. (currently amended) A method as recited in claim 1 5, wherein the step of applying Table

15   Mask operation includes employing permutations for index and/or data values formed by

16   composing several individual permutations.

17   17. (currently amended) A method as recited in claim 1 5, wherein the step of applying the Table

18   Mask operation includes employing several individual permutations to defeat at least one

19   higher-order side-channel attack.

20   18. (original) A method as recited in claim 1, wherein said at least one table is a table from an

21   application of General Countermeasure Against Side-channel Attacks.

22   19. (original) A method comprising:

DOCKET NUMBER: YOR20010711US2   **5/25**

Serial No.: 09/943,720

1   providing a lookup table for a data processing operation;

2   performing a table split operation upon said lookup table in forming a collection of split
3   tables;

4   performing a table mask operation upon said collection of split tables and/or upon other
5   lookup tables in forming a plurality of masked tables;

6   performing a table aggregate operation on at least two of said plurality of masked tables
7   in forming at least one aggregate table; and

8   performing said data processing operation on a combination of split, masked, aggregate
9   and lookup tables.

10   20. (original) A method comprising:

11   providing a data processing operation involving at least one lookup table, each particular
12   table from said at least one lookup table having a particular lookup table size and a particular
13   lookup table index size;

14   declaring any lookup table from said at least one lookup table to be splittable:

15   if the table lookup size of said any lookup table is larger than an amount of RAM
16   available, or

17   if the table index size of said any lookup table is larger than available addressing
18   capability;

DOCKET NUMBER: YOR20010711US2   **6/25**

Serial No.: 09/943,720

1   performing a table split operation upon said any lookup table declared splittable in the
2   step of declaring and forming a collection of split tables;

3   performing a table mask operation upon said collection of split tables and/or other of said
4   lookup tables forming a plurality of masked tables; and

5   performing said data processing operation on a combination of split, masked, aggregate
6   and lookup tables.

7   21. (original) A method as recited in claim 20, further comprising performing at least one table
8   aggregate operation on at least two of said plurality of masked tables forming at least one
9   aggregate table.

10   22. (original) A method as recited in claim 21, wherein the step of performing said data
11   processing operation includes performing a table aggregate operation whenever a total size of all
12   masked tables exceeds an amount of RAM available.

13   23. (original) A method as recited in claim 21, wherein the step of providing includes obtaining
14   the data processing operation.

15   24. (original) A method as recited in Claim 20, wherein the step of performing a table split
16   operation includes employing an Output Divisor Table Splitting Method.

17   25. (original) A method as recited in Claim 20, wherein the step of performing a table mask
18   operation includes employing an Input-Output XOR Permutation Masking Method.

19   26. (original) A method as recited in Claim 21, wherein said table aggregate operation includes
20   employing a Byte-wise XOR Aggregate Method.

DOCKET NUMBER: YOR20010711US2   **7/25**

Serial No.: 09/943,720

1   27. (original) A method as recited in claim 21, further comprising performing said data

2   processing operation on a combination of split, masked, aggregate and lookup tables.

3   28. (original)   A method as recited in claim 20, further comprising employing the data

4   processing operation as a countermeasure against at least one side channel attack.

5   29. (original)   A method as recited in claim 1, wherein a number of elements in said at least one

6   lookup table is 200.

7   30. (original) An article of manufacture comprising a computer usable medium having computer

8   readable program code means embodied therein for causing resistance to side-channel attacks,

9   the computer readable program code means in said article of manufacture comprising computer

10   readable program code means for causing a computer to effect the steps of claim 1.

11   31. (original) An article of manufacture comprising a computer usable medium having computer

12   readable program code means embodied therein for causing resistance to side-channel attacks,

13   the computer readable program code means in said article of manufacture comprising computer

14   readable program code means for causing a computer to effect the steps of claim 19.

15   32. (original)   An apparatus comprising:

16   means for declaring any lookup table from a provided set of lookup table to be splittable

17   if the table lookup size of said any lookup table is larger than an amount of RAM available, or if

18   the table index size of said any lookup table is larger than available addressing capability, each

19   particular table from said set of lookup tables having a particular lookup table size and a

20   particular lookup table index size, said any lookup table;

21   means for performing a table split operation upon said any lookup table declared

22   splittable in the means for declaring and forming a collection of split tables;

DOCKET NUMBER: YOR20010711US2   **8/25**

Serial No.: 09/943,720

1   means for performing a table mask operation upon said collection of split tables and/or

2   other of said lookup tables forming a plurality of masked tables; and

3   means for performing said data processing operation upon a combination of split,

4   masked, aggregate and lookup tables.

5   33. (original)   An apparatus as recited in claim 32, further comprising means for performing a

6   table aggregate operation on at least two of said plurality of masked tables.

7   34. (original)   An apparatus as recited in claim 33, wherein the means for performing a table

8   aggregate operation performs the table aggregate operation when the total size of all masked

9   tables exceeds the amount of RAM available.

10   35. (original)   An apparatus as recited in claim 32, wherein the means for declaring obtains said

11   any lookup tables from another module.

12   36.. (currently amended) A method comprising

13   providing a data processing operation involving a first lookup table in a cryptographic

14   process, said lookup table having a first lookup table size;

15   creating a randomized table in which entries or indices are statistically independent of

16   entries or indices of said first lookup table, said randomized table having a randomized table size

17   being smaller than said first lookup table size, wherein the step of creating said at least one

18   randomized table includes applying a Table Split operation to at least one of said lookup tables

19   resulting in split lookup tables; and/or applying a Table Masking operation to at least one of said

20   lookup tables and/or split lookup tables resulting in masked tables, and wherein the step of

21   applying a Table Split operation includes employing a Two-way Byte Table Splitting Method;

Serial No.: 09/943,720

1   employing said randomized table for securely handling information in said cryptographic

2   process;

.3   prior to performing the cryptographic process, transforming the information by applying a

4   secret-sharing operation to the elements of the information where each element of the

5   information is related to multiple elements of the transformed information;

6   performing the cryptographic process on the transformed information involving the use of

7   said randomized table; and

8   retransforming the transformed and cryptographically processed information by applying

9   an inverse secret-sharing operation to the transformed and cryptographically processed

10   information.

11   37. (original)   A method as recited in claim 36, further comprising performing said data

12   processing operation employing said randomized table.

13   38. (original)   A method as recited in claim 36, wherein said cryptographic process is performed

14   in a cryptographic information processing system or device.

15   39. (original)   A chip card comprising a module implementing the steps of claim 1.

16   40. (original)   A method as recited in claim 1, wherein said at least one lookup table is fixed.

17   41. (currently amended)   An apparatus comprising:

18   a randomizer module to create at least one randomized table in which entries and/or

19   indices are statistically independent of entries and/or indices of any table from a provided set of

20   lookup tables, each individual table from said at least one randomized table having a randomized

21   table size, wherein:

DOCKET NUMBER: YOR20010711US2   **10/25**

Serial No.: 09/943,720

1   a first sum of sizes of all said randomized tables is smaller than a second sum of

2   sizes of all said at least one lookup tables, or

3   the maximum index size of said randomized tables is less than the maximum

4   index size of the lookup tables; and

5   a processing module to perform said data processing operation employing said first

6 randomized table, wherein said at least one randomized table applies a Table Split operation to at

7 least one of said lookup tables resulting in split lookup tables; and/or applies a Table Masking

8 operation to at least one of said lookup tables and/or split lookup tables resulting in masked

9 tables, and wherein the Table Split operation employs a Two-way Byte Table Splitting Method.

10 42. (original) An apparatus as recited in claim 41, wherein the randomizer module forms said

11 provided set of lookup tables.

12 43. (original) An apparatus as recited in claim 41, wherein the randomizer module includes a

13 splitting module to perform a Table Split operation upon at least a subset of said set of lookup

14 tables resulting in split lookup tables.

15 44. (original) An apparatus as recited in claim 41, wherein the randomizer module includes a

16 masking module to perform a Table Masking operation upon at least a subset of said set of

17 lookup tables and/or split lookup tables forming a set of masked tables.

18 45. (original) An apparatus as recited in claim 43, wherein the randomizing module includes an

19 aggregating module to perform a Table Aggregate operation to at least one masked table.

20 46. (original) An apparatus as recited in claim 43, wherein the splitting module includes an

21 Unequal Table Splitter Module which applies the Unequal Table Split Method for performing a

22 Table Split Operation.

DOCKET NUMBER: YOR20010711US2   **11/25**

Serial No.: 09/943,720

1   47. (original) An apparatus as recited in claim 44, wherein the masking module includes an

2   Input-Output XOR Permutation Masking module which applies the Input-Output XOR

3   Permutation Masking Method for performing a Table Mask Operation.

4   48. (original) An apparatus as recited in claim 45, wherein the aggregating module includes an

5   Byte-wise XOR Aggregating Module which applies the Byte-wise XOR Aggregating Method for

6   performing a Table Aggregate Operation.

7   49. (original) A computer program product comprising a computer usable medium having

8   computer readable program code means embodied therein for causing resistance to side-channel

9   attacks, the computer readable program code means in said computer program product

10   comprising computer readable program code means for causing a computer to effect the

11   functions of claim 32.

12   50. (original) An apparatus comprising

13

14   a splitting module to perform a table split operation upon a provided set of lookup tables,

15   forming a plurality of split tables;

16   a masking module to perform a table mask operation upon said collection of split tables

17   and/or other lookup tables forming at least one masked tables;

18   an aggregating module to perform a table aggregate operation on a subset of said plurality

19   of masked tables, forming at least one aggregate tables; and

20   a processing module to perform a data processing operation employing a combination of

21   split, masked, aggregate and lookup tables.

DOCKET NUMBER: YOR20010711US2   **12/25**

Serial No.: 09/943,720

1   51. (original) An article of manufacture comprising a computer usable medium having

2   computer readable program code means embodied therein for causing resistance to side-channel

3   attacks, the computer readable program code means in said article of manufacture comprising

4   computer readable program code means for causing a computer to effect the steps of claim 20.

5   52. (original) An article of manufacture comprising a computer usable medium having

6   computer readable program code means embodied therein for causing resistance to side-channel

7   attacks, the computer readable program code means in said article of manufacture comprising

8   computer readable program code means for causing a computer to effect the steps of claim 36.

9   53. (original) A program storage device readable by machine, tangibly embodying a program of

10 instructions executable by the machine to perform method steps for causing resistance to

11 side-channel attacks, said method steps comprising the steps of claim 1.

12 54. (original) A program storage device readable by machine, tangibly embodying a program of

13 instructions executable by the machine to perform method steps for causing resistance to

14 side-channel attacks, said method steps comprising the steps of claim 20.

15 55. (original) A program storage device readable by machine, tangibly embodying a program of

16 instructions executable by the machine to perform method steps for causing resistance to

17 side-channel attacks, said method steps comprising the steps of claim 36.

18 56. (original) A computer program product comprising a computer usable medium having

19 computer readable program code means embodied therein for causing resistance to side-channel

20 attacks, the computer readable program code means in said computer program product

21 comprising computer readable program code means for causing a computer to effect the

22 functions of claim 41.

23 57. (original) A computer program product comprising a computer usable medium having

24 computer readable program code means embodied therein for causing resistance to side-channel

DOCKET NUMBER: YOR20010711US2   13/25

Serial No.: 09/943,720

1   attacks, the computer readable program code means in said computer program product

2   comprising computer readable program code means for causing a computer to effect the

3   functions of claim 50.